BLACKOUT WARFARE

Cyber-Attacking Electric Power Grids: A New Strategic Weapon

Dr. Edward M. Roche
EMP Task Force on National and Homeland Security
July 4, 2021

TABLE OF CONTENTS

KEY JUDGMENTS

The United States faces imminent danger from a devastating cyber-attack against its electric power grid. This attack is more probable because a Revolution in Military Affairs has weakened the deterrence traditionally associated with conventional and nuclear weapons, changed the escalation ladder, and consequently lowered the barrier to intensive conflict between the superpowers.

A new form of cyber-attack against the electric grid has emerged in the form of a "non-shooting" war between Nation States. This type of attack might take place between superpowers as something that is short of use of conventional or nuclear force.

There is a popular myth that cyber weapons can be made "by any teenager in a basement using software downloaded from the web." This is not at all true if we consider the target. It is not everyone who can write the specific code needed to disable an electric power grid. Apart from the programming skills, they need to have superb knowledge of the grid itself, how it works, and the specific equipment being made the target of the attack. They must understand the operational procedures of the specific facility being targeted.

Russia is the best prepared to defend against cyber-attack and use cyber as a strategic weapon. During an extreme international crisis, a massive Russian cyber-attack against the entire U.S. electric grid prior to the outbreak of conventional or nuclear war is likely, to deter or defeat the U.S. with "gray-zone aggression" instead of or prior to outbreak of a "real shooting war": consistent with Russia's military doctrine that Cyber Warfare is an unprecedented and decisive Revolution in Military Affairs.

China is likely to make a massive cyber-attack against the entire U.S. electric grid prior to the outbreak of conventional or nuclear war, or during an extreme international crisis, to deter or defeat the U.S. with "gray-zone aggression" instead of or prior to outbreak of a "real shooting war": consistent with China's military doctrine that Cyber Warfare is an unprecedented and decisive Revolution in Military Affairs.

Iran has a moderate chance of inflicting temporary but substantial damage to the electric grid, primarily in its supporting information processing operations. It is unlikely that Iran would be capable of cyber-attacking the entire electric power grid of the United States.

The Non-State Actor does not have the capabilities of a superpower, or of any Nation State. It lacks the engineering skills, money, and infrastructure to develop a cyber-weapon as complex and sophisticated as Stuxnet. Cyber-attacks by Non-State Actors against the entire U.S. electric grid are an unlikely event. Cyber-attacks against regional (or city) electric grids are more probable but would be unsophisticated and primitive.

For U.S. relations with both Russia and China, the emergence of viable paths to cyber-attacks against critical infrastructure as a new strategic weapon has lowered the barriers to conflict, and presents a heightened danger with the potential to disrupt the long-standing balancing calculus dependent upon nuclear deterrence.

BLACKOUT WARFARE
Cyber-Attacking Electric Power Grids: A New Strategic Weapon

Background

The United States faces imminent danger from a devastating cyber-attack against its electrical grid. This attack is more probable because a Revolution in Military Affairs has weakened the deterrence traditionally associated with conventional and nuclear weapons, changed the escalation ladder, and consequently lowered the barrier to intensive conflict between the superpowers.

In April 2021, Russia massed troops on Ukraine's border apparently threatening an invasion, raising alarms in the U.S. and NATO. Ventriloquizing for the Kremlin, Putin intimate and director of Russia's state-run international media giants, RT and Sputnik, Margarita Simonyan, in a TV interview declared:

"Russia will invade Ukraine, sparking a conflict with the U.S. that will force entire cities into blackouts…All-out cyber warfare, nation-wide forced blackouts."[1]

"War is inevitable," according to Russia's Simonyan, "I do not believe that this will be a large-scale hot war, like World War II, and I do not believe there will be a long Cold War. It will be a war of the third type: the cyber war."[2]

Russia's Simonyan:

--"In conventional war, we could defeat Ukraine in two days. But it will be another kind of war. We'll do it, and then [the U.S.] will respond by turning off power to [a major Russian city like] Voronezh."
--"Russia needs to be ready for this war, which is unavoidable, and of course it will start in Ukraine."
--Russia is "invincible where conventional war is concerned, but forget about conventional war…it will be a war of infrastructures, and here we have many vulnerabilities."
--"I've been agitating and even demanding that we take Donbas [eastern Ukraine]. We need to patch up our vulnerabilities as fast as we can, and then we can do whatever we want."
--"We only lose if we do nothing," agreed Russian TV interviewer Vladimir Soloviev. "He argued that by absorbing parts of Ukraine—or the entire country—Russia would be able to remove the zone of American influence further from its borders," reports Julia Davis.[3]

Russian TV described cyber-attack options ranging from small-scale to existential threats, including: blacking-out part of New York City (Harlem was mentioned), or blacking-out the state

[1] Julia Davis, "Top Kremlin Mouthpiece Warns of 'Inevitable' War with U.S. Over Another Ukraine Land Grab" www.thedailybeast.com (13 April 2021).

[2] Ibid.

[3] Ibid.

of Florida, or blacking-out the entire continental United States. To defeat the U.S., according to Russia's Simonyan: "We don't even need the nukes."[4]

Just weeks after the above Russian cyber-threats, in May 2021, the U.S. Colonial Pipeline was hacked, shutdown temporarily. Cyber-attacks can destroy pipelines, causing them to explode. Colonial Pipeline is crucial to fueling U.S. military power projection capabilities from the east coast to protect NATO, or to help Ukraine, during a Russian invasion.[5] That is why the Colonial Pipeline was really targeted, not for the millions paid in ransom, but as a demonstration of Russia's cyber-power.

The Colonial Pipeline cyber-attack proves Russia is not bluffing.

Moscow's Cyber War knockout blow—blacking-out U.S. electric grids and other critical infrastructures, has been planned for years:

--March 2016, U.S. Government Joint Technical Alert warned Russia's cyber-attack Dragonfly: "Targeted government entities and multiple U.S. critical infrastructure centers, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."[6]
--2017, the Department of Homeland Security (DHS) disclosed, as headlined by Wall Street Journal and Newsweek: "Russian Hackers Could Have Caused Electricity Blackouts In The U.S."[7]
--March 2018, Reuters reported: "Senior U.S. intelligence officials said…the Kremlin believes it can launch hacking operations against the West with impunity." Russia "staged malware…and gained remote access into energy sector networks."[8]
--July 2018, DHS warned of Russian cyber-penetrations into hundreds of U.S. electric utilities. These cyber-attacks were probably the simulated "tip of the spear" for VOSTOK-18, a major joint Russia-China strategic exercise held in September 2018, practicing World War III.[9]
--December 2020, DHS disclosed Russia's Solar Winds cyber-attack penetrated 18,000 U.S. Government and private sector agencies and corporations, including the Defense Department and U.S. Cybersecurity and Infrastructure Security Agency. Damage is still being evaluated.[10]

On Sunday, April 11, 2021, the world woke up to alarmist complaints by Iran without proof blaming Israel for an attack on its electrical grid. Power supplying its Natanz nuclear processing facility disappeared. At the same time, newspapers in Israel were boasting that a cyber-attack

---

[4] Ibid.

[5] "When Will America Protect Itself Against EMP, Cyber and Ransomware Attacks?" The Hill (21 May 2021).

[6] Dustin Volz and Timothy Gardner, "In A First, U.S. Blames Russia For Cyber Attacks On Energy Grid" Reuters (15 March 2018). CISA, Alert TA18-074A (15 March 2018) us-cert.cisa.gov/ncas/alerts/TA18-074A

[7] Jason Murdock, "Russian Hackers 'Could Have Caused Electricity Blackouts' in the U.S." Newsweek (24 July 2018).

[8] Dustin Volz and Timothy Gardner, "In A First, U.S. Blames Russia For Cyber Attacks On Energy Grid" Reuters (15 March 2018).

[9] Dr. Peter Vincent Pry "Understanding VOSTOK-18" originally published as "The Danger of Russia's Largest Military Exercise" Newsmax Platinum (8 October 2018) danhappel.com.

[10] Terry Thompson, "The Colonial Pipeline Ransomware Attack and the SolarWinds Hack Were All But Inevitable" news.yahoo.com (10 May 2021).

engineered by its scientists and secret service had been responsible for this disaster.[11] Of the three parts to the electricity grid –a) Generation; b) Transmission; and c) Distribution – here the attack had been on the distribution side. An "electrical substation located 40 to 50 meters underground" was destroyed. "[T]housands of centrifuges" used to separate Uranium-235 from Uranium-238 had been put out of service, at least temporarily.[12] The strategic implications were grave. An electrical grid was being used as a strategic weapon to impede Iran's path in violation of its obligations under the Nuclear Non-Proliferation Treaty towards creation of an atomic bomb.[13] Here, interference with the electrical grid was used not to disrupt Iran's economy and society, but instead to injure a strategic military facility with pinpoint accuracy. As the press continued to reverberate the story, discussion widened to consider cyber-attacks as a means of war.

According to the Office of the Director of National Intelligence:

"Cyber threats from nation states ... will remain acute. Foreign states use cyber operations to ... damage ... physical ... critical infrastructure. ... [W]e remain most concerned about Russia, China, Iran, and North Korea."[14]

From 1965--2020 there were 68 blackouts in the United States affecting 100,000 or more persons for at least 1 hour and comprising at least 1,000,000 person-hours of disruption. Can a cyber-attack be used to turn an electrical grid into a strategic weapon? If so, then what type of planning would need be done by a rival effectively to harm the United States?

Attacking Electric Grids—A Tool Of Strategic Conflict

The United States is a superpower. Even its enemies know it should not be attacked lightly. There must be a reason, and that reason must fit into the grand strategy of the attacker. At the heart of the matter is "why?". What is the strategic logic? What type of international crisis would be severe enough to drive a rival Nation State to launch a major cyber-attack against America's electrical grid? We know that motivations vary, and so do the capabilities and boldness of attackers. For the

[11] Subsequent analysis showed that the disruption to the power supply in Natanz was caused not by cyber, but by setting off an explosion underground to destroy a transformer. This was done by somehow recruiting an individual to carry out this attack. Nevertheless, the world's press continued to circulate the story, shifting to more general arguments about the vulnerability of the grid. *See* Yonah Jeremy Bob, Lahav Harkov, Tzvi Joffre "Mossad behind attack on Iran's Natanz nuclear facility" The Jerusalem Post online (13 April 2021 10:12):"Western sources said the facility was hit by a cyberattack, but The Jerusalem Post learned that it was a confirmed physical attack."

[12] Tzvi Joffre, Yonah Jeremy Bob, "Natanz nuclear site blast: Iranian State TV identifies man behind attack" The Jerusalem Post (17 April 2021 13:44) *quoting* Iranian officials. The bomber was identified as Mr. Reza Karimi. What is surprising is that the Iranian government presented an "Interpol Wanted" card on the bomber, meaning that he had been able to carry out the bombing and get out of Iran. *It is likely the cyber-attack story had been a smoke screen to allow the bomber to escape from Iran*. Note in particular there are not "thousands" of centrifuges in that facility.

[13] Iran still was learning that no Nation State has a "right" to build this type of weapon.

[14] Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community*, p. 20 (9 April 2021 *hereinafter* "ODNI 2021 Rpt").

time being, however, let's assume the reason is there. If this is the case, then the question becomes "What *type* of cyber-attack?"

Of course there are different levels of attack, ranging from small irritating skirmishing actions to a major attack aimed at taking out electrical power for a region of America or a single large metropolitan area. At the top extreme is an all-out attempt to disable the nation's entire electrical grid aiming to plunge the country into a chaotic and horrifying darkness. For a small Nation State, it is doubtful they could assemble enough capability successfully to launch a cyber-attack nationwide against such a giant electrical grid in its entirety. One of America's rival superpowers could.

Cyber-attacks by tradition are broken down into two classes. One type is the "supplementary" variety, the other is "stand-alone". In the supplementary form, cyber-attacks are used to assist projection of military force. Cyber becomes one of many tools in a military confrontation. The highest priority targets usually are the command and control systems of the enemy's military. Only if the conflict reaches a higher level of intensity does it become a possibility to engage civil society targets. If there were cyber-attacks on both military and civilian targets, and these were being deployed as a supplement to national military force, then this would mean the parties were engaged in a "Total War."[15] This is the highest and most unfortunate level of conflict, but if we follow the traditional and accepted concepts regarding nuclear deterrence this scenario is unlikely between the superpowers. Under traditional strategic defense theory, all-out cyber conflict would take place only as an adjunct to either conventional or nuclear war.

Does this logic still hold? What about other types of attack? In the stand-alone form, cyber-attacks are launched from one Nation State to another *without* being a supplement to ongoing use of conventional or nuclear military force. These are "cyber-only" attacks. Not associated with a declared war, they often are anonymous. After all, a weaker attacker does not wish for a stronger power to know they are the source of the problem, because this would expose them to retaliation. To avoid a such a response, the smaller fry tend to "fly under the radar" in an effort to hide in the dimly lit vastness of cyberspace.

A new form of cyber-attack against the electrical grid has emerged in the form of a "non-shooting" war between Nation States. This type of attack might take place between superpowers as something that is short of use of conventional or nuclear force. Some argue that "non-kinetic" cyber-attacks are not an "armed attack" under international law and thus there is no right given to a Nation State for self-defense under Article 51 of the United Nations Charter.[16] Consequently, they argue, this lowers the chance of kinetic retaliation. With less to worry about, the result has been a perceived relaxation of inhibitions governing the use of cyber-attacks by Nation States. For example, one observer has stated that under some circumstances, Russia might take steps to injure the American electrical grid in response to a move by the United States in support of the

[15] *See* Erich Ludendorff, *Der Totale Krieg* (München: Ludendorffs Verlag, 1935); Definition: Total warfare a war that is unrestricted in terms of the weapons used, the territory or combatants involved, or the objectives pursued, especially one in which the laws of war are disregarded. (*Oxford Reference*).

[16] This legal catfight never has been satisfactorily resolved.

Government of Ukraine. Such a scenario might happen in this sequence:[17] a) The separatist areas of Eastern Ukraine become involved in an internal fight with their Government; b) When violence escalates, Russia moves in to protect the majority Russian-nationality population, which perhaps is demanding a plebiscite on breaking away from the Ukraine and becoming an independent state or joining Russia; c) The United States makes the mistake of intervening in this civil war and launches a cyber-attack against the electrical grid *of Russia* or parts of it, such as a city; d) Having been attacked, Russia *always* responds, so it launches a counter cyber-attack against the mainland of the United States and takes out an equivalent part of the American Electrical Grid.

According to a commentator on Russian state television:

"I do not believe that this will be a large-scale hot war, like World War II, and I do not believe that there will be a long Cold War. It will be a war of the third type: the cyberwar."[18]

The damage inflicted would be short of conventional or nuclear war, and as expected for reckless national security advisors who have not seen real war, the barriers to adopting a strategy expressed as a cyber-attack against the electrical grid consequently would seem to be lower. *This is a new development in strategic defense theory.* It envisions a central war between the superpowers without resorting to conventional or nuclear forces. Instead, they will rely on cyber-attacks.

Cyber Has Automated Espionage

Cyber has automated espionage. It now is hundreds of thousands of times more effective than any other type of spying.[19] Intelligence gathering[20] is aimed at both the opponent's Civil Society and government, including its military forces. Since the mid-1990s, a massive amount of information has been exfiltrated from even our most highly-protected and "secure" targets. The pilfered information covers a comprehensive range of topics including military, technological, political, industrial, strategic, personnel, and others. Cyber espionage has more than proven its worth. It is "cost effective." This would be beautiful in another context, but here, it is the United States that has been the victim harmed the most. A paradox of cyber is that the most advanced Nation States are the most vulnerable to attack with this quirky and asymmetric weapon.

For the purpose of understanding cyber-attacks against the electrical grid, we must note an important sub-class of espionage – the practice of gathering up technical intelligence regarding the networks and interconnected devices within the territory of one's opponent. At first, this sounds like a giant and overwhelming assignment, particularly if one is considering mapping and making sense of the networks within an entire Nation State. Indeed it is that. Nevertheless, with the use

---

[17] *See* statements of Margarita Simonyan and Vladimir Soloviev on Russian state television, *reported by* Julia Davis "Top Kremlin Mouthpiece Warns of 'Inevitable' War With U.S. Over Another Ukraine Land Grab : 'Don't Even need the Nukes'" www.thedailybeast.com (13 April 2021).

[18] Margarita Simonyan quoted by Davis, Ibid.

[19] Human Intelligence (HUMINT); SIGINT; MASINT; ELINT, etc.

[20] In many models, this part of the process is referred to as "Reconnaissance", but that term refers to electronic surveillance of the network inside an organization once it has been penetrated, it is a *sub-set* of intelligence gathering.

of automation, it is in fact possible to map such giant infrastructures, and even develop a database that contains basic information about many if not all of the connected devices.[21] Of course with technological developments such as the Internet of Things (IoT),[22] and IPv6,[23] the number of inter-connected devices theoretically can approach 10^{27} devices *per person*, yet this vast number also is within the range of automated mapping.

Apart from the technological wizardry of automated mapping, this form of espionage has an important and serious function. It makes it possible to pinpoint the best targets to attack. Automated mapping can locate the Internet-connected control devices in an electrical grid. Once that is done, the identity of these critical devices can be determined. Their identity known, internal cyber-dependent components can be dissected. When a hacker knows how something works, they can figure out how to stop it from working.

Next, malware can be created, then *inserted* into the foreign infrastructure. In some cases, such malware is designed merely to be there in case it is needed. It remains dormant. This is a type of pre-positioning that allows a Nation State to have code ready inside the infrastructure of an opponent. It is safe to assume that the infrastructure of the United States has been mapped, penetrated, and is full of pre-positioned code from enemies ready to strike.[24]

Even if there is no pre-positioning of malware, the use of cyber intelligence to identify key electrical grid control technologies has enabled enemies to write code that can be used to turn these devices into the equivalent of bombs.

Choice Of Cyber-Attack Vectors Depends On The Target

No matter what their underlying purpose, there are different types of cyber-attacks. Some are indiscriminate; others aimed at specific targets. Here, we assume that an attack against the

[21] There are many examples. *See* Internet-map.net.

[22] The Internet of Things (IoT) describes the network of physical objects–"things, or objects"–that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

[23] Internet Protocol Version 6 is vastly increasing the number of Internet addresses, and thus the number of possible interconnected devices. By 1998, the Internet Engineering Task Force had formalized the successor protocol. It designed IPv6 to use a 128-bit address, theoretically allowing 2^{128}, or approximately 3.4×10^{38} addresses. The old IPv4 used a 32-bit address space and allowed for 2^{32} unique addresses.

[24] There have been "multiple intrusions into US ICS/SCADA and smart grid tools [to] ... gather[] intelligence [and] develop capabilities to attack." *See* Timothy M. Wintch, "Perspective: Cyber and Physical Threats to the U.S. Power Grid and Keepng the Lights On" Homeland Security Today (20 April 2021) *quoting* Mission Support Center, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, Idaho National Laboratory, 22 (2016), 22; There are rumors the United States has pre-positioned destructive dormant code into the electrical grids of its rivals, but this is impossible to determine with any reliability.

electrical grid would be targeted, not indiscriminate. This narrows down the types of attack that might be used. For example, an indiscriminate DDoS[25] attack would be ruled out.[26]

A targeted attack against an important national security asset such as the electrical grid would require a number of phases. The target must be identified and its function understood. Preparation must be made, and a strategy for getting access to the target must be worked out. That being accomplished, the attack may be launched. Let us look at this in greater detail.

Pre-Attack Intelligence Gathering Selects The Target

Depending on the target, intelligence collection may be easy or difficult, or perhaps impossible.

Luckily for its enemies, the United States is one of the world's softest intelligence targets. An analyst's dream. So much information is freely available. In the Chi Mak Spy ring, for example, the spies found that in order to handle the pilfered technical information stolen from Boeing, it was necessary to rent multiple vans to drive the boxes upon boxes of documentation down to the Chinese Consulate in San Francisco.[27] *Truckloads* of information, and that using the old fashioned "brick and mortar" type of espionage.

There are other important sources. Leaks abound. In the "Game of Thrones" cut-throat winner-takes-all environment of Washington, D.C., U.S. Government employees seeking to further one agenda or another routinely leak highly technical and strategically sensitive information, usually making it available over the World Wide Web. In the cyber world, the Government itself routinely publishes details on important computer exploits whereupon hackers use this information to conduct their work. America's industries also contribute to the softening process because they like to publicize their accomplishments and sales. As a consequence, when everything is added together, this ocean of information available in the United States gives an incomprehensible advantage to rivals. Go to a country such as Russia, and the situation is completely different. Information that Americans consider as being routine there is kept out of sight.

When getting ready for an attack, analysis of cyber intelligence goes through a narrowing-down process. First, there is an extended general scan of the environment. Here, it would involve probing and compiling an analysis of the target Nation State as a whole. At some point, a decision is made to hit the Electrical Grid.[28] After that, then cyber espionage becomes more specific. It narrows down collection activities to thoroughly examine the nature of the specific target. For the

---

[25] Distributed Denial of Service (flooding a server with so many requests that it becomes over-loaded, thus making it impossible for regular customers/visitors to receive its service)

[26] A more restrictive model is the "Cyber Kill Chain" developed by Lockheed Martin. It involves a) Reconnaissance (harvesting email addresses, conference information, etc.); b) Weaponization (Coupling exploit with backdoor into deliverable payload); c) Delivery (Delivering Weaponized bundle to the victim via email, web, USB, etc.); d) Exploitation (Exploiting a vulnerability to execute code on victim's system); e) Installation (Installing malware on the asset); f) Command & Control (C2) (Command channel for remote manipulation of victim); and g) Actions on Objectives (With "Hands on Keyboard" access, intruders accomplish their original goals).

[27] *See* Edward M. Roche, *Snake Fish: The Chi Mak Spy Ring* (New York: Barraclough Ltd., 1996).

[28] The electrical grid could be the sole target; or merely one of many targets.

electrical grid in the United States, it would take only a short period of time to determine the gigantic scale of the network, and its organization into multiple units such as the a) Western Electricity Coordinating Council; b) Southwest Power Pool; c) Texas Reliability Entity; d) Reliability First Corporation; e) SERC Reliability Corporation;[29] f) Northeast Power Coordinating Council; and g) Florida Reliability Coordinating Council.

In an electrical grid, there are four major cyber systems that can serve as targets for attack including a) Supervisory Control and Data Acquisition Systems (SCADA) responsible for managing real-time measurements from substations and sending controlling signals to equipment such as circuit breakers or other control systems; b) Substation Automation Systems which are tasked with control of local equipment (in a single facility); c) Energy Management Systems responsible for real time analysis of the reliability of systems, usually by taking continuous samples of propagating electricity waves, *e.g.*, monitoring of frequency; and d) Market systems that are responsible for buying and selling of electricity on both a bulk and consumer basis, including the spot market. The highest priority for a cyber-attack is the SCADA equipment. These can turn off the power and possibly trigger a cascade of blackouts.[30]

Any of these systems provide a rich environment for launching a cyber-attack. For example, a Substation Automation System (SAS) links together in a network many substation devices including a) Intelligent Electronic Devices (IED); b) Network (ethernet) switches; c) Database and application servers; d) Front-End Processors (communications equipment that links an information system to one or more networks); e) Telecommunications gateways (equipment that links one network to another and sometimes translates from one protocol to another); and f) Workstations for engineers and operators, sometimes referred to as the "HMI" or "Human Machine Interface."[31]

For a modestly sized system designed to provide 1,500 MW of power, the Substation Automation System will need to be capable at a minimum of processing 50,000 data points streaming in from more than 600 Intelligent Electronic Devices (IEDs).

It is popular to use the IEC 61850 communication protocol. Switchgear has numerical relays on this standard and the breakers are managed through the Distributed Control System (DCS).[32] A large amount of information travels back and forth reporting on the a) Status of the system components (circuit breaker open/close; circuit breaker in a testing routine or in service; motor speed switch); b) Protection data (breaker positions; thermal warning; Load-jam trip element; Phase under-voltage; breaker operation count); and c) Important measurement data (R-, Y-, and B-phase current; RYB Voltage and frequency; power; phase current measurements).[33]

---

[29] Four organizations in the Southeast – the CARVA Pool, Tennessee Valley Authority (TVA), Southern Company, and the Florida Electric Power Coordinating Group – combine to form SERC.

[30] For an example of a cascading blackout, see below a description of the recent Texas blackout.

[31] *See* Saroj Chelluri, Diego Rodas, Ala Harikrishna "Integration Considerations for Large-Scale IEC 61850 Systems" 2nd Annual Protection, Automation and Control World Conference (Dublin 27-30 June 2011).

[32] A DCS has high reliability because control processing is distributed to different nodes in the system, instead of having a single processor that might take down the entire system.

[33] Ibid.

Since these all are crucial factors for understanding the operation of the power plant, should these reporting data points be disturbed, there is a risk of power interruption. In addition, if these data points could be intercepted then the status of plant operations could be made to look different from what it actually is. Many of these systems also are part of an underlying alarm system, and if disabled would nullify any tip-off to plant operators of a problem.

For example, proud engineers describing operation of the Indira Ghandi Super Thermal Power Project in Jajjar announced to the world a serious potential vulnerability in their plant: *"Modern numerical relays ... capture all feeder data, report events, monitor the equipment ... Such near real-time data of the complete auxiliary system ... displayed on a human-machine interface (MHI) help monitor the system from remote locations."*[34]

Unfortunately, should these data paths be set up for remote access, there is a potential cyber-security problem because hackers can "dial in" and do their sabotage. This is what happened in the 2015 Ukraine incident.

The standard for delay in getting signals from these devices is 10 milliseconds or less.[35] The access to the Intelligent Electronic Devices (IED) is through the Ethernet switches which feed the SCADA servers and the Operator workstations.

How might this Intelligence analysis work? A network analysis, based on widely-available scanning tools, would reveal that the electrical grid of the United States could be broken into half with ten targeted attacks along a vertical line north from the mid-way point between El Paso and Tucson. Furthermore, by study of documents such as the North American Electric Reliability Corporation (NERC)[36] Critical Infrastructure Protection (CIP) Standards[37] for the Bulk Electric System[38] it would be easy to identify all of the cyber defense activities underway at each major facility. For an enterprising hacker, it might be possible to penetrate the information system of the NERC and obtain copies of the self-studies and assessments benchmarking the CIP Standards as well as details of Reliability Standard Violations. This would quickly lead to the IEC 61850 standard of the International Electrotechnical Commission.[39] This, in turn, would lead to the detailed knowledge found in documents such as a) IEC TR 61850-90-1:2010 for communication between substations; b) IEC TR 61850-90-2:2016 for communication between substations and

[34] Ibid.

[35] Ibid. (noting that delay for CAT 5e/6 cables is 0.55 milliseconds per 100 meters; for fiber optics 0.49 and for wireless 0.33)

[36] North American Electric Reliability Corporation (NERC). Created by the U.S. Government and designed to protect part of the electricity infrastructure of the United States.

[37] These standards apply specifically to the cybersecurity of the Bulk Electric System.

[38] Bulk Electric System (BES): Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. *See* NERC, *Bulk Electric System Definition Reference Document*, Ver. 3 (August 2018).

[39] Work of its Technical Committee 57.

control centers; c) IEC TR 61850-90-5:2012 for transmission of synchrophasor information;[40] and d) IEC TR 61850-90-7:2013 for power converters in distributed energy resources (DER) systems.

Knowing the equipment to target and its possible vulnerability is insufficient. It is necessary to know the precise IP address of the equipment on the *internal* network of the facility. It may be necessary to exfiltrate this data after gaining preliminary access into the local system. In the Lockheed cybersecurity model, this is called the "Reconnaissance" phase.

For example, according to the E-ISAC Ukraine Report on Russia's cyber-attack on the Ukraine electric grid: *"After the attackers achieved the necessary freedom of movement and action in the IT infrastructure, they began exfiltrating the necessary information and discovering the hosts and devices to devise an attack concept to hijack the SCADA DMS to open breakers and cause a power outage."*[41]

Intelligence analysis would be able to find the location of all active Phasor Measurement Units.[42] Perhaps by using review of the trade press, the attacker would correlate the sales of IEC standard compliant equipment to various utility companies (and their locations). Perhaps it would target synchrophasor sites. Or perhaps it would target a Schweitzer Engineering Laboratories Software Defined Networking installation to *increase* its "Deny by Default" architecture response time from <0.1milliseconds to >0.5ms or even to >30ms. That should do it. There are many options to choose from.

Initial determination of the preferred scale of a cyber-attack is essential. Luckily for the attacker, they can determine that the electrical grid in the United States is subject to a cascading blackout effect. It is riddled with critical points that if disturbed will produce a chain reaction of one blackout causing another which in turn causes another. This was seen on August 10, 1996 in the Northwest United States (7.5 million customers), and August 14, 2003 in the Northeastern United States and Canada (50 million customers).[43]

Cascades happen because as each line is shut down, the electricity must be moved over to another transport route. "A line *overloads* if the absolute amount of power flowing in it exceeds a given

[40] Synchrophasor is a device (Phasor Measure Unit or PMU) that estimates the size and phase angle of an electrical phasor quantity (voltage; current) using a common time source for synchronization. It measures the frequency in the power grid. Typical measurement is 120 times per second. A phasor ("phase vector") is a complex number incorporating (1) amplitude (A); (2) angular frequency; and (3) initial phase.

[41] *See* Robert M Lee, Michael J. Assante, Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid" E-ISAC (18 March 2016) p. 15, para. 5.

[42] *See* for example "The three different D[istribution] M[anagement] S[ystem] vendors were discoverable via open-source searching." *in* Robert M Lee, Michael J. Assante, Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid" E-ISAC (18 March 2016) p. 10, fn. 28 (*hereinafter* "E-ISAC Ukraine Report" describing the identification of technology used in Ukraine in 2015).

[43] *See* Ian Dobson, "Cascading Network Failure in Power Grid Blackouts," *Encyclopedia of Systems and Control* (London: Springer-Verlag, 2014).

line threshold." This leads to an immediate "outage of the corresponding line."[44] So if the electricity is passed over to a line without the capacity, the circuit will shut down, merely as a safety measure.

The potential for cascading blackouts in the electrical grid in the United States is a gift to the enemy. It would not be necessary to disable all of the utilities, or transmission switching points across the country. Instead it should be possible to damage the United States, its economy and its people merely by locating the handful of points that would cause a cascade of power failures.

Simulations have confirmed this approach. For example, a study in 2005 found that "an efficiency loss (damage) of up to 25% is possible after the loss of a *single* generator or transmission substation".[45] Another study of cascading effects in the electrical grid found that merely one-fifth of all failures were primary, and the rest were secondary, that is, they were caused by a blackout somewhere else on the network, usually next door.[46] The study found that larger cascades can be generated by an attack of multiple nodes that are close to each other, and close to the vulnerable set:

"[There is a] set of network components that are vulnerable to cascading failures under any out[age] of multiple conditions. ... [T]he vulnerable set consists of a small but topologically central portion of the network ... [L]arge cascades are disproportionately more likely to be triggered by initial failures close to this set. ... [L]arge cascades tend to be triggered by perturbations adjacent to the set of 'early adopters'."[47]

Here, the term 'early adopters' refers to parts of the grid that have blacked out first. Once these vital points in the electrical grid are identified, then the intelligence work can be focused on penetration of their supporting facilities. In the United States these vulnerable points in the electrical grid have been identified, but surprisingly do not appear to have been made public. Nevertheless, we must assume that through espionage, enemies have stolen copies of these classified studies and know precisely where to hit.

Intelligence collection also might focus on the personnel at target locations. Providing the Nation State has the resources, this information might lead to a recruitment or other inducement to cooperate on the part of persons with access to the facility. Over a long time, agents might be placed in key facilities.

---

[44] *See* Tommaso Nesti, Alessandro Zocca, and Bert Zwart "Emergent Failures and Cascades in Power Grids: A Statistical Physics Perspective" 120 Physical Review Letters 258301-1 (2018).

[45] *See* R. Kinney, P. Crucitti, R. Albert, V. Latora "Modeling Cascading Failures in the North American power grid" European Physical Journal B, Vol. 46 (2005) pp. 101-107, ("[T]he first node removed does the most damage while each successive removal does little to the worsening of the average efficiency. Similar behavior is recorded for generators." p. 106, para. 2).

[46] *See* Yang Yang, Takashi Nishikawa, Adilson E. Motter "Small Vulnerable Sets Determine Large Network Cascades in Power Grids" 358 Science, eaan3184 (2017).

[47] Ibid., p. 5

The final work in the intelligence phase would be an analysis of the effects of a cyber-attack. Would it disable an intended target, such as a manufacturing plant, or military base? What would be the response from the target Nation State if the attacker were identified? Since this part of the analysis is little more than sophisticated guesswork, it will go quickly.

Nevertheless, the primary outcome of the intelligence phase of this operation would be an identification of the targets as well as the most promising technique for launching a successful cyber-attack that would have the desired effect. The bad news is that this work likely already has been done by enemies.

A Cyber Weapon Is Built With A Payload And Vector

In the next phase of the operation the attacker must a) build the cyber weapon; b) determine how to get it delivered; c) continue to assess the downstream effects of its use; d) develop contingencies for the operation if things do not go as planned.

The effect of a cyber-attack could be either less serious than anticipated, or could become much larger than anticipated. At the same time, intelligence monitoring if possible should continue to detect any material changes in underlying conditions, either technology-wise, politically, or as a detectable change in levels of security at a targeted site.

The most important part of the preparation phase is building the malware ("cyber-weapon") that will be used. Cyber weapons are similar to a biological virus; there are two crucial components. A virus such as Covid-19 has two essential elements. First, the RNA to be injected into the cell allowing it to cause replication of the virus itself. Second, a pathway ("vector") must be available to pass the RNA into the target cell. Any cyber weapon malware also has two essential components. First is the "payload." This refers to the [computer] code that will carry out the operations of the malware. In Stuxnet, the payload software was responsible for harming the centrifuges in Natanz, Iran. Second, the "Vector." This refers to the "exploit" that will be used to inject the damaging code into the target information system. Exploits are a "bug" in the operating system, applications or connected firmware-controlled devices. It can be exploited to sneak in the payload undetected.

There is much remarkable creativity in writing exploits. The recent SolarWinds attack used a novel vector of being put into commercial software *before* it was distributed from the factory to customers.[48]

[48] *See* Dina Temple-Raston, A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack" NPR website (16 April 2021). In attribution of the attack, the author writes that it was "Hackers *believed to be* directed by the Russian intelligence service" responsible (Emphasis Added). There is no indication regarding the identity of who believed the attack to originate in Russia and why they came to this conclusion. This means that attribution to Russia is either the product of analysis by U.S. intelligence services, or propaganda posing as a "leak" to feeder journalists. It is impossible to tell. All we know is that no evidence has been presented. How would someone know the precise details of how the SVR *in Russia* was directing a group of hackers *in Russia*? (SVR ``Sluzhba vneshney razvedki Rossiyskoy Federatsii", Foreign Intelligence Service of the Russian Federation).

Sourcing of these two components is completely different. For the most part, exploits ("vectors") for delivery of a payload may be obtained on the Dark Web ("Black Market") where they are auctioned off to the highest bidder. These markets operate with anonymity, or at least give the appearance of doing so. If these exploits are not yet known to the vendors of the software, they are given the name "Zero Day" exploits.[49]

Design of the payload is more complex. Here, the code must be written to the precise specifications that will accomplish the sabotage intended. To do that, the hacker must first obtain a realistic testbed to use for ensuring the software will work.[50] A diverse and skilled workforce is needed. It is a team effort, not that of an individual. There must be programming talent, but also knowledge of electricity, and operation of the grid, and also knowledge of the specific engineering characteristics of the device that is going to be penetrated and manipulated to inflict the intended damage.

There is a popular myth that cyber weapons can be made "by any teenager in a basement using software downloaded from the web." This is not at all true if we consider the target. It is not everyone who can write the specific code needed to disable an electrical grid. Apart from the programming skills, they need to have superb knowledge of the grid itself, how it works, and the specific equipment being made the target of the attack. They must understand the operational procedures of the specific facility being targeted.

For example, in the Stuxnet malware used to inhibit illegal uranium refinement (separation of U-235 from U-238) in Iran, the United States went through a number of steps including a) Interception on the high seas of identical gas centrifuges that were being shipped from North Korea to Libya; b) Transportation of the seized equipment to one of its national laboratories, probably Oak Ridge; c) Setting up the centrifuges and getting them to operate so they could be studied and used as a test bed; d) Intensive study of the SCADA systems controlling the equipment; e) Development of an attack plan for the malware (the attack was meant to remain hidden, so the centrifuges would appear to break randomly and naturally); f) Development of a systems design plan to create the software to do the intended task; g) Extensive testing of the malware; h) Intensive surveillance of the target facility in Iran for the purpose of determining the method for delivering the malware; i) Acquiring the Zero-Day exploits to serve as vectors for the malware payload; then j) Final Testing.

If the discovery and forensic analysis of Stuxnet is any guide, the programming expertise for its development required at least two separate domains of computer science including a) Traditional programming familiar with operating and networking systems of standard ICT equipment; and

[49] Once an exploit is discovered (or purchased) by the vendor, they quickly rectify the vulnerability, and issue an update ("patch") to their software. After that, the countdown for the exploit begins. As days go by, users around the world gradually come to install the update on their system. When they do this, then the value of the malware decreases. Not everyone patches their system on a timely basis. So even if a particular exploit is known, and a solution issued in an update, still there always remain a large number of users who are negligent in doing the update. As a consequence, they remain vulnerable.

[50] *See* "The adversaries likely had systems *in their organization* that they were able to evaluate and *test their firmware against* prior to executing on December 23rd." E-ISAC Ukraine Report, p. 10, para. 5 (Emphasis Added).

b) Specialized machine programming of the SCADA systems, written in different languages, and relying on a generally separate set of skills.

This does not even account for all of the required engineering knowledge of how to operate a centrifuge. Apart from all of that extensive effort, there was a significant intelligence activity put into place including both collection, and either development or preparation of the human networks that would be used to introduce the malware into Iran. If those activities are added to the bill, and considering the intelligence work plus the engineering work, Stuxnet was probably a billion dollar weapon.

In sum, this was the type of work that could have been done only by a Nation State and definitely *not* by someone in a basement using off-the-shelf malware purchased from the sleaze merchants lurking on the Dark Web.

Obtaining Site Access Requires Intelligence Resources And Analysis

The next phase may just as well start up as the preparation phase is winding down. In order to accomplish this type of penetration of a sensitive electrical grid facility, the attacker can use a variety of tried and trusted techniques.

There are two methods of access for a cyber weapon. First, it can be introduced through the general Internet. If the systems being attacked are on the web, then they might come under attack. Spearphishing is the most common way hackers are able to get a foothold inside a target system. But security experts long have been aware of this problem and as a consequence have dis-connected many critical machines from the open Internet. This is done by setting up small Internets using the same underlying technology and standards, but with no gateways to the outside world. If this happens then a common way to cross this "air gap" is through an employee of the facility (or visitor) that might take in the malware on their own laptop or on a USB drive. One of the famous stories in this regard is the Nation State that placed invisible malware on USB drives, then scattered them in the parking lots of Department of Defense employees, whereupon these were picked up, taken into the facilities, and then plugged in so the curious (the unwitting "vector") could see their content. Once plugged into a network, the malware escaped into the closed system and the air gap had been breached.

There are other access techniques as well. These include a) Recruitment of human resources inside the facility;[51] b) Penetration of the facility with an operative using some form of social engineering (pretending to be someone they are not); c) Rigging of equipment shipped into the facility; or d) Some other method not known.[52]

[51] Recruitment of human is done through the MICE framework: Money, Ideology, Blackmail or Ego. *See* Randy Burkett "An Alternative Framework for Agent Recruitment: From MICE to RASCLS" 57 Studies in Intelligence 7 (2013)

[52] *See* "[I]t is likely that the adversary will modify attack approaches in follow-on campaigns and these mitigation strategies may not be sufficient". E-ISAC Ukraine Report, p. 14, para. 1.

All of these techniques for delivery of the malware take extensive resources, surveillance, analysis and sophistication. It is possible that extensive training would be required, raising further the complexity and barriers inhibiting a cyber-attack.

Cyber-Attacking The Electric Grid May Have Multiple Objectives

Finally, the time arrives to conduct the attack. The way this occurs is dependent on the larger theatre of conflict. In its simplest sense, the attack must be seen within the context of other parallel actions – political, diplomatic, military, economic – taking place at the same time. Here, the most fundamental distinction is whether or not a cyber-attack against the electrical grid takes place as a stand-alone effort, or is within the context of a larger conflict involving conventional or nuclear weapons. In the Gulf Wars, cyber was used extensively to "soften up" the Iraqi targets before actual kinetic attacks were launched. In this classical model, exploitation of the vulnerabilities in information systems was merely one of many tools used by the military in conducting its compelling work.

Under the new strategic defense logic, it is possible that a cyber-attack against America's electrical grid might be fired off as a stand-alone event. Russia's reported repeated attacks on the Ukraine electric grid, and China's blackout of Mumbai, India, are attacks of this sort. Much depends on the overall political context, and the goals of the attacker. Stand-alone attacks could be aimed at accomplishing a number of goals including a) Doing damage to a specific region of a Nation State, perhaps one that is symbolic, such as the nation's capital; b) Sending a "warning signal" to deter some current or feared action by the Nation State being attacked; c) As punishment for a real or perceived confrontation with the attacker Nation State;[53] or d) As a prelude or diversion in preparation for an attack elsewhere.[54]

Lessons Learned From Past Cyber-Attacks Against Electric Grids

In the United States, cyber-attacks represent a major threat to the electrical grid.[55] Hackers have a number of types of equipment they can target including a) Supervisory Control and Data Acquisition (SCADA) systems; b) Emergency Management Systems, including the Energy Control System, Transmission Management System, and Generation Management System; c) Distributed Control Systems (DCS) found at generating plants; d) Substation Automation Systems, located at transmission substations; and e) Distribution Automation systems, found at distribution substations or on distribution pole tops. Most of these are connected using the Internet protocols.

---

[53] When there was a collision off the coast of China between a recklessly driven Chinese fighter jet and a U.S. reconnaissance aircraft, and also when there was an accidental bombing of the Chinese embassy in Yugoslavia (7 May 1999). NATO bombing. Operation Allied Force. Location: Belgrade: 3 killed 27 injured. There was a fierce cyber-attack against the United States launched by so-called "patriot hackers" in China.

[54] This list is by no means complete.

[55] *See* Marcus H. Sachs "Securing the North American Electric Grid" Lecture, RSA (Rivest-Shamir-Adelman) Conference, San Francisco (13-17 February 2017).

The World's First Cyber-Attack On Critical Infrastructure

In December of 2015, the Ukraine suffered a number of cyber-attacks across its society.[56] One of the attacks went after its electricity power grid.

The electrical grid in the Ukraine is composed of more than 14,230 miles of High Voltage Lines and 135 Substations. In 2015 the consumption of electricity was as high as 187 TWh.[57] The peak load of the system was around 32GW.[58] It was powered by 14 Thermal plants (102 units of 800-150MW); 4 nuclear plants (15 units 1000-440MW); 7 Hydroelectric plants (94 units 117-19MW); 3 Pumped Storage facilities (9 units 325-37MW) and 3 Cogeneration plants (9 units 250-100MW). There appears to be a single large junction approximately at Uman linking the East with the West of the country.

On December 23, 2015, the electrical power plant servicing Ivano-Frankivsk, Ukraine, suffered a cyber-attack. Seven (7) 110 kV substations, and twenty-three 35 kV substations had been disconnected:[59]

"We started receiving calls from different regional energy operators, which was a surprise because they were not connected on the grid. It meant that something unusual was happening. When we looked at our computers, we saw that the mouse cursors were moving by themselves, randomly, and were disconnecting the power from different substations, disconnecting switchers, lines and transformers. What to do? We received information there was external interference."[60]

This cyber-attack left 225,000 Ukrainians without electrical power. The attackers used privileged access. They corrupted ICS systems in both the control room and field and wiped (erased) servers throughout the IT environment. All of this was accomplished without the need for even one attacker to set foot inside the facility. The steps in conducting the attack were are follows: a) Spear

[56] December 6th (Ministry of Finance; State Treasury; State Pension Fund); December 12th (State Executive Service; Internet Service Provider Volya); December 13th (Defense Ministry); December 14-15 (Railways); 16th (Ministry of Infrastructure); 20th (Sea Port Authority; Stock Exchange).

[57] Terawatt-hour (TWh) is 10^{12} Watt-Hours.

[58] GW is Gigawatt or 10^{9} Watts.

[59] Data from Kyivoblenergo. This name is an abbreviation for "Kiev Region Energy Organization" [Kiev-Oblast-Energia-Organizatsi].

[60] NATO, What Happens When a Power Plant Comes Under Cyber Attack?, Video, Interview with Bohdan Soicuk, Operational Dispatcher Service, Prykarpattyaoblenergo Power Plant, 2016.

Phishing;[61] b) Establish persistent remote access;[62] c) KillDisk;[63] d) Credential Harvesting;[64] e) VPN Hack;[65] f) Learn Operations;[66] and g) Attack.[67] These are described below:

Like all Spear Phishing campaigns, it started with an innocent official-looking document sent out from an official-sounding email address. The email began "In accordance with the Presidential Decree 15/2015" which is the standard opening for an official document in the Ukraine. It then goes on to mention national "mobilization" to "strengthen the Ukraine."[68] The malware was a macro inside a Microsoft Office document. Once the attachment was opened, the malware was injected, thus infecting the endpoints in the information system.

This gave the attackers a compromise of the workstations in three electricity distribution control centers.[69] Once inside, the next step was to harvest the access credentials (login and password information). These included both credentials from the local workstations, but also those used for remote access[70] to the SCADA systems. With this access, the attackers installed malware in the SCADA systems.

At the same time, the attackers disabled the uninterruptible power supply protecting the control centers. Later on, when the control room employees were attempting to restore their systems, there was no power.

Next, corrupt firmware was uploaded and put on the Serial-to-Ethernet gateways in the substations. These are the gateways that take sensing information from equipment and put it on the Ethernet on its way to the Human Machine Interface used on the workstations of the operators. Once this bad firmware was installed, the gateways were blocked, making it impossible for anyone trying later to get the electricity turned back on remotely to close the breakers, because those commands would not go through. To "close" a breaker means to connect the circuit allowing electricity to flow.

---

[61] Targeted systems administrators at local utility companies; (the attackers pretended to be either vendors or government employees).

[62] Installation of RATs ("Remote Access Trojan") to establish backdoor access.

[63] Attackers then installed "KillDisk" malware, making it possible to overwrite most files upon command of the attacker, thus rendering the system un-bootable.

[64] The attackers then guessed and stole credentials until they were able to obtain an administrator ("admin") credentials ("Credentials Harvesting").

[65] Attackers captured Virtual Private Network credentials; this allowed them remote access into control room systems without having to be inside the facility.

[66] Using this access, the attackers monitored operations for weeks, learning how the system was operated.

[67] After understanding the system, the attackers executed a highly coordinated attack.

[68] Author's translation.

[69] Note that this Phishing attack was being conducted throughout the Ukraine, not only against Electricity Grid targets.

[70] "Remote Access" is used when a worker wishes to access their workstation from the outside, such as when they are working at home.

Once the access was verified, then an operator connected in from the outside using the compromised remote access system. They logged in and then shut down the power by opening the circuit breakers. This was an option in "dialogue mode" for an operator. An "open" breaker means that the circuit is cut. Using this technique, the power in every substation was shut down.

Since by now the breakers could no longer be closed by remote commands (the firmware upload had blocked this capability), the only way to restore power was to send actual repair personnel to the substations to manually close the breakers allowing the electricity once again to flow, thus losing much time.

The SCADA system in the control room then was taken down by more cyber malware. This was done using a "wiper" program, one that erases all of the data on a machine. Once the data was erased from a system, the situation could have been saved by using a backup program and re-installing all of the system. But here, that could not happen because the power had been cut, and its backup, the uninterruptible power supply, had been put out of service. Remember that cutting the power also had cut the power to the control center itself.

The attack had enabled the attackers to disconnect electricity breakers and cut power in regions across Ukraine. They also were able to lock out the control room operators from their own software, making it impossible for them to do their work.[71]

This was an artful attack because it was able to use the existing SCADA control system to shut down the power with the credentials of an authorized operator. Merely gaining control of the workstations and the credentials had been sufficient. In a sense, this was a less sophisticated attack than one that might have involved use of special malware to corrupt the SCADA systems and cause them to operate in an unpredictable way. This had happened at Natanz in Iran from the StuxNet malware attack. But in the Ukraine, during this attack, the SCADA systems operated correctly—it was the false commands from the hijacked workstations that were the source of the problem.

The nature of the cyber-attack tells us something about the attackers. It is clear that detailed thought was given into not only turning off the power, but also on making it difficult for the operators to *restore* it. In order to conduct this operation, the attackers would have had to know the restoration procedures, and perhaps have gamed out the attack at a test facility. The remote attacker posing as a legitimate operator would by necessity have been trained on operation of the system. They would need to know how to issue the right commands and how to read the display. If the attackers were operating from any part of the former Soviet Union, it might have been easier for them to have obtained this training on a parallel testbed, since the Ukraine uses primarily Russian equipment for its electricity grid.[72]

This event, the world's first cyber-attack against a critical infrastructure facility could have been prevented if the Ukrainian company had put into practice a number of well-known precautions

[71] *Source*: CyberArk "Threat Analysis: The Ukraine Shutdown" Video (23 March 2017).

[72] This is mere speculation, but plausible.

including a) Protecting against the Spear Phishing attack, which is one of the most commonly used ways of getting malware into target information systems; b) Setting of strict segregation of the IT network from the SCADA network using either a total separation approach or implementation of a DMZ.[73] (This would have prevented the attackers going through the network and installing the "Wiper" software on the SCADA system.); c) Either completely blocking any remote access to the system or improving the security of remote access through actions such as two-factor authentication, and the requirement that any remote access session be approved *each time* by local staff, (sensitive facilities probably should allow zero remote access; none whatsoever); d) Adding well-known network security controls for the Serial-to-Ethernet gateways by using either a firewall or an access control list which, for example, would have blocked the TCP port that was used for firmware uploads (The "Boreas" vulnerability);[74] e) Not having their Uninterruptible Power Supply connected to their network, because that is how the hackers disabled the power supply, leaving the control room dark when it should have been working on recovery of systems.[75]

It is regrettable that all of the above security precautions were well-known at the time, and they would have been effective, at least against this particular cyber-attack.

In essence, this plan involved a) Taking complete control of the Control Room systems; b) Then opening breakers, disabling the uninterruptible Backup Power Supply; updating the firmware in substations to disable communications so that afterwards no one would be able to issue restore commands; and activating the KillDisk malware throughout the IT environment causing erasure of workstations; and as icing on the cake; and c) Launching a telephone Denial of Service Attack that would prevent customers from reporting outages. It was altogether a professional and well-executed cyber-attack and obviously was meant to send a "signal" to the Government of the Ukraine. This perhaps was a type of "demonstration" attack. In a real conflict, one assumes the blackouts would have been much more extensive.

So in addition to the Ukraine electrical grid attack being the "world's first cyber-attack against critical infrastructure" it also was the "world's first use of an electrical grid blackout to send a powerful diplomatic signal."[76]

---

[73] In computer security, a DMZ or demilitarized zone ("perimeter network"; "screened subnet") is a subnetwork that limits exposure of internal network parts to the outside. Outsiders can access only what is exposed. Other things are hidden.

[74] *See* discussion in Goce Kiseloski, Dobre Blazhevski, Veno Pachovski "Protecting Power Grids: Will There Be Light In The Future" Working Paper, School of Computer Science and Information Technology, Skpoje, noting: "The vulnerability of ICS devices has its roots decade ago. U.S. Department of Homeland Security identified vulnerability in ICSs back in 2007 dubbed Boreas. This vulnerability allows permanent disabling controllers by simply loading manipulated firmware." (undated). *See also* Ralph Langner *Stuxnet und die FOLGEN* Hamburg: Langner Communications GMBH (August 2017) p. 38 para. 1.

[75] *Source*: Langner Group.

[76] This assumes the intention to carry out the operation truly was from Russia and the overall context involved the tense situation in the Eastern Ukraine, which is of vital strategic importance to Russia.

The Texas Blackout Shows What Can Happen And How Fast

A sketch of how a power grid disaster in the United States would work is found in the February 2021 blackout in Texas. It was caused by severe cold weather, and eventually left 4.5 million homes and businesses without electric power. Texas operates around 46,500 miles of electricity transmission lines connected with around 5,000 substations. It relies on a single balancing authority,[77] and is interconnected via only two links to other grids because it wishes to maintain independence from the Federal Government.[78] It receives almost one-half of its power from burning natural gas (51,667 MW, 47.45%). Surprisingly, Texas is a relatively "Green" state as it gets 31,390 MW from Wind (28.83%). Other sources include 13,630 MW (12.52%) from coal, 5,153 MW (4.73%) from nuclear and 6,177 MW (5.67%) from the Sun. Each of these different sources of electrical energy act differently when subjected to extreme weather.

Within an 8-hour period on February 15th, the Texas grid lost 15 GW of power from natural gas, and lost 3 GW from wind. The wind farms did not perform well in the poor weather. Coal eventually lost around 5,000 MW. Nuclear and solar also lost some power, but their shares are insignificant compared to natural gas.

Initiating the crisis was the demand for electricity which grew dramatically because for many it was the primary means of keeping warm. For various reasons, starting on February 15th, the amount of generation capacity *unavailable* increased dramatically. It quickly jumped from 30,000 MW up to 55,000 MW and remained there until the middle of the 17th at which point it started slowly to decrease. By the 20th, it had been reduced to approximately 29,000 MW *unavailable* for use.

In the United States, the electrical grid must operate at 60~cycles per second. Of course there is some variation allowed. As more electricity is demanded, it causes a decrease in the frequency of the grid. Unless there is a massive sudden change, the actions of individuals, or even buildings is not noticeable. The frequencies of the electricity being generated are carefully monitored, as this data is used to ramp up or ease off the amount of electricity generated. In a simple sense, as more people turn on their electric heaters, the frequency is pulled down, this is sensed, and the generators are ordered to increase production. These adjustments happen within seconds. It is not unlike "plate spinning."[79]

It is a marvel of engineering that this happens across the giant electrical grid and the granularity of the measurements are in the milliseconds. On February 15th in Texas, the grid frequency went up to a little more than 60.1 (cycles per second) at around 1:26 in the morning. By 1:42 am it had dropped back down to 60.0, the standard rate. The term electricity companies use for turning off the power is "Load Shedding". By 1:45 am, only three minutes later, the frequency had dropped

[77] A balancing authority ensures, in real time, that power system demand and supply are finely balanced. The Electric Reliability Council of Texas (ERCOT) covers most, but not all, of Texas and consists of a single balancing authority. *Source*: U.S. Energy Information Administration.

[78] The United States has approximately 60 balancing authorities.

[79] "Plate spinning" is a circus manipulation art where a person spins plates, bowls and other flat objects on poles, without them falling off.

to 59.88, and this triggered a "Load Shed" order at around 1:47 am. Load shedding is a major event for an electricity utility because it means that power is being cut to customers.

Who gets their power cut? There is a system of prioritization, so certain critical facilities, such as hospitals, may remain connected to the grid. But a family living in their house will be cut. After all, most persons were sleeping at the time.

Unfortunately, this cut in power was not enough. The demand for electricity continued to jump up, thus pulling down the frequency of the grid, as more power was demanded. By 1:51 am, the frequency had dropped below the critical frequency of 59.4 cps. This is a type of "red line" for the grid, because as the frequency continued to drop from 60 cps, the electrical generation activity of the power station was rising to compensate, but at 59.4 cps, the maximum generation capacity of the power plant is reached, and it turns off as a safety measure in order to prevent damage to itself. To stop this, the response must be immediate Load Shedding, and that is what happened.

At 1:55 am, the grid frequency still was operating at 59.32 cps, dangerously low. So this massive shutdown of parts of the Texas grid had happened in a little less than nine minutes.

Demand for power continued to pull down the grid frequency and it remained in the 59.32 cps range through four more minutes, until 1:55 am at which time a *third* Shed Load order was executed. At that point, the grid frequency started to recover and by 1:57 it was in the 59.7 range, and by 1:59 it was at the 59.95 cps level, at which point a *fourth* Shed Load command was executed! By 2:01-2:02 am the frequency was still in the 59.5 range but by 2:03 it had recovered fully to 60cps and by 2:05 was up to 60.19 cps. The severe Shed Load orders had been executed between 1:51 to 1:59 am.

Only 8-9 minutes had been required to trigger the blackout.

The Load Shedding had allowed the total generation capacity of the grid to drop from 71,000 MW on the evening of February 14th to approximately 48,000 MW (-32%) the evening of the 15th where it stayed until mid-day on the 17th, when it rose again by the next day to around 65,000 MW. The Load Shed at first was small, but by the second order had jumped to 10,000 MW. It then rose to around 18,000 MW and hit as high as 20,000 MW the evening of the 15th and mid-day on the 16th. By the 17th, it was falling but remained at around 15,000 MW mid-day, then fell to zero by mid-night on the morning of the 18th.

The economic impact on the electricity industry was substantial. Between February 13th and 19th, the spot price for natural gas went up from a three-year average of less than $5 per MMBtu[80] to more than $230 dollars per MMBtu. This was a severe disruption to the market for natural gas.

This change in the availability of electricity also had a substantial effect on its marketing. In Texas, as elsewhere, different companies supplying the grid purchase electricity from each other on an

[80] MMBTU is Million British Thermal Units (BTU); 1 BTU is the amount of heat required to rise the temperature of one pound of water by one degree Fahrenheit.

"as needed" basis. The prices remain generally low, but they are dynamically adjusted according to demand. If there is a "spike" in demand, then the spot price for wholesale electricity will go up. This is accounted for on a regular basis, as companies buy back and forth from each other, and reconcile periodically. On February 13th, the Texas Wholesale Electricity Spot Price jumped up to $1,000 per MWh.[81] It then quickly jumped as high as $8,900 per MWh which is an extraordinarily high price. By the 14th it was back down to the $900–$1,000 range, but then as night fell it jumped back up to $2,000, then $5,500, then $8,900 again. On the 15th, the price dropped for a short while to $4,000, but quickly jumped back up to $8,950. As the Load Shedding actions were undertaken, the spot price dropped back down as low as $1,500 but that evening jumped back up to the "ceiling" of $9,000 *and remained at that level* until the afternoon of the 19th at which time it dropped back down to a little above zero, which is the customary rate. For some facilities that had contracts to pay for electricity at a "market rate" instead of a fixed rate, they were subjected to some "Sticker Shock" when they received their electricity bills.

The lesson from Texas is that the electricity grid is more fragile than perhaps one may think. Out of range events such as an untoward surge in demand can cause a cascade of blackouts. It also indicates that an enemy attack against the U.S. electric grid would take place ideally in very cold weather, when electricity demand is at its highest. This would increase the chance of a catastrophic failure.

The Mumbai Blackout Confirms the Threat of Pre-Positioned Malware

India and China have a border dispute in India's North East. Some of the problem has its origin in the break-up of India and the spin-off of Pakistan in 1947.[82] In 1963 territory to the east of the Karakoram Range bordering Ladakh and Baltistan was ceded by Pakistan to China, but this was not recognized by India. This is the source of the border dispute. The problem stems from China's attempts unilaterally to seize Indian territory. A tense stand-off eventually led to several Indian deaths at the hands of the invading Chinese. Why these two great nations would have a military conflict over this desolate and unpopulated wasteland is difficult to understand. The conflict has been simmering for decades.

As the conflict and argumentation intensified, Chinese hacker groups developed a plan for a cyber-attack on India's power grid. In keeping with commonly used penetration techniques, the hackers set up a number of typosquat[83] domains. These were mimics of the domain names for Indian electrical power companies. For example, NTPC Limited is an Indian company in the electricity supply business. The typosquat used the the hackers was ntpc-co.com whereas the genuine web address was ntpc.co.in. There were at least 15 domains registered this way, and most were hosted by the same company HKBN Enterprise Solutions HK Limited. Three were hosted by

[81] MegaWatt Hour.

[82] The British Indian Empire was partitioned into the Dominion of India and the Dominion of Pakistan.

[83] The term "typosquat" is a combination of Type and Squat. In Internet parlance, squatting is taking hold of the domain of another, and then refusing to release it until paid. It generally refers to a domain name that is similar enough to the targeted domain that the two easily are confused. Type (typo) refers to the way which squatting takes place, which is by slight modification of a protected domain name. An example of a typosquat would be Update-Microsoft.com or Microsofts.com.

EHOSTICT, another company in China.[84] The registrations were made by WEBCC, which offers registration for a number of domains such as ".cc", ".cn", ".sg", ".tw" and a number in Chinese characters such as ".香港"(xianggang) (Hong Kong), and ".公司" (gongsi.xianggang) (Company, Hong Kong).[85] The domains were registered through eznowdns.com, an "uncommon authoritative name server."[86]

The function of these installations was to work as Command and Control (C2) servers that direct malware covertly pre-positioned in target information systems. C2 servers work approximately in this sequence a) An exploit is found to load malware into a target information system; b) Once the malware is in position, it collects information about the host system it has infected; c) The malware then sends out signals to the C2 server; these signals contain important information about the targeted system (location; type of applications; name; other characteristics); d) The C2 server then "decides" if the target system shall become a target for attack; e) If yes, then the malware is sent a signal to activate; f) If activated, then the malware module begins to download and execute further malicious code to do things such as exfiltrate data, erase all of the data in the information system, change important settings, steal credentials, etc.[87] g) If not, then the malware remains sleeping and perhaps at some point erases itself.

If the presence of the malware within the target system is not known, nevertheless this type of operation may be detected when the concealed malware sends out its signals to the C2 server.[88] At some point in the host environment, the signal must pass through a router. But routers can be trained to look for specific IP addresses or even for IP addresses that are not "ordinary." For example, if the process within the host system in India generally is designed to interact with workstations within its facility, then why would a packet of information be heading out the door to an unknown server registered in Hong Kong?

---

[84] It is not known when these domains were first operational.

[85] Using pinyin for romanization.

[86] *See* analysis by Insikt Group, *Cyber Threat Analysis China*, White Paper, Recorded Future, Doc. No. CTA-CN-2021-0228, *hereinafter* "Insikt Rpt.". *NB:* A name server refers to the server component of the Domain Name System (DNS), one of the two principal namespaces of the Internet. The most important function of DNS servers is the translation (resolution) of human-memorable domain names (example.com) and hostnames into the corresponding numeric Internet Protocol (IP) addresses (93.184.216.34), the second principal name space of the Internet which is used to identify and locate computer systems and resources on the Internet.

[87] *See* Kaspersky "ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World" cyber news blog at kaspersky.com: "Following the installation of an infected software update, the malicious module would start sending DNS-queries to specific domains (its command and control server) at a frequency of once every eight hours. The request would contain basic information about the victim system (user name, domain name, host name). If the attackers considered the system to be 'interesting,' the command server would reply and activate a fully-fledged backdoor platform that would silently deploy itself inside the attacked computer. After that, on command from the attackers, the backdoor platform would be able to download and execute further malicious code."

[88] *See* Insikt Rpt., ("Using a combination of proactive ... infrastructure detections, domain analysis, and ... Traffic Analysis" p. 1).

Attempts are made to avoid this type of detection, and this is done by spacing out the signals to only 2-3 per day, and from a data point of view, these are very small messages, probably encrypted. But this type of flying under the radar does not always work.

The advantage of this type of "scatter seeds then evaluate" approach for the attacker lies in the lack of discrimination in the initial attack. Rather than being forced to do the extensive research in advance to find the precise cyber-locations[89] of the target systems, one may merely spew out a giant attack all over the Internet, and this attack may have little if any need for discriminating between systems before infecting them. In the Mumbai power matter, the attackers were using ShadowPad, which is a "backdoor planted in a server management software ... used by hundreds of large businesses around the world."[90] The software was planted in NetSarang[91] technology. It was possible for someone to determine that there were a large number of IPs resolving to Indian critical infrastructure.[92]

It appears that these China-based C2 servers were able to pre-position malicious software on "10 distinct Indian power sector organizations, including 4 of the 5 Regional Load Dispatch Centres ... responsible for operation of the power grid."[93] This happened at approximately the same time as Indian soldiers were fighting off encroachments from invading Chinese troops near Chushul. In May of 2020, the tense stand-off resulted in the first combat deaths between China and India in 45 years.

On October 13, 2020, the electricity failed in central Mumbai. It happened in the center of the vibrant business district. Train and emergency services had their electrical power disrupted. The stock exchange itself managed to continue operation, most likely because it had reserve back-up power, but its trading volume took a nose dive. The power outage started at 10 am and lasted for two hours. At this time, the Covid crisis was at its peak in Mumbai, and as hospitals lost power, there was a sudden wave of fear and panic. The power outage had hit India's financial capital, and surrounding areas.

An investigation by Tata Power later determined there was a simultaneous tripping of circuits at two substations, Kalwa and Kharghar. This caused a large dip in grid frequency in the Mumbai transmission system and led to a cut off of the power supply.

The Maharashtra Government investigated the blackout and concluded it was the result of cyber sabotage. Its Home Minister, Anil Deshmukh provided a briefing based on a confidential report concerning the blackout incident:

---

[89] IP Addresses.

[90] *See* Kaspersky "ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World" cyber news blog at kaspersky.com.

[91] Netsarang Computer at www.netsarang.com. This was discovered in July, 2017 by Kaspersky Lab.

[92] Insikt Rpt., Ibid.

[93] Insikt Rpt. *assessing that* "Pre-positioning on energy assets may support several potential outcomes, including geo-strategic signaling during heightened bilateral tensions, supporting influence operations, or as a precursor to kinetic escalation."

"Fourteen Trojan Horse malware [programs] may have been installed in the server. Similarly, 8 GB [of] unaccounted data may have been transferred from [a] foreign server. ... Many blacklisted IP Firms may have tried to log into [Indian power] server[s]."

The research had been done by Ernst & Young working with a cybercrime unit of the Maharashtra government.[94] The 100-page preliminary report from the cybercrime unit depicted three potential sabotage methods, a malware attack on the server of the Maharashtra State Electricity Board (MSEB), a transfer of 8 GB of unaccounted data from a foreign server to the MSEB, and attempts by several blacklisted IP addresses to login into the MSEB server.

After the attack, it was reported that the Central Electricity Authority sent out alerts informing operators that 40 sub-stations had detected malware entering their information systems. India's Computer Emergency Response Team (CERT-In) reported that Command and Control (C2) servers in China were making contact with systems in the Telangana State Load Dispatch Centre. It identified the presence of the ShadowPad malware. Later India's National Critical Information Infrastructure Protection Centre (NCIIPC) issued a warning pointing to a Chinese state-sponsored group and circulated a list of IPs and registered domains that should be blocked. It advised all power utilities to take protection and safety measures. The Indian operators dutifully took the list of Chinese C2 servers and reconfigured their firewalls to shut them out. As part of the house-cleaning, all of the control centers on the electricity grid not only blocked the listed IPs and domains, they also scanned all of their software to search for any installed malware. Some installations removed discovered malware from their systems. Their firewall settings then were strengthened even further. In addition, other protective measures were put in place.[95] India is re-evaluating its use of Chinese-manufactured equipment in its grid.

It was not the first incident. The Telangana power system had been attacked previously by hackers in April of 2019. Their Greater Hyderabad service area had been subjected to a ransomware incident.[96]

The message was clear. Shutting down an electricity grid is a possibility for China in its attacks on India. In diplomatic terms, the two-hour blackout was considered by many to be a "warning" to India.

Attacks On America's Grid Will Come From Nations And Terrorists

The type of cyber-attack that may be launched by an opponent against the United States also varies with the capabilities of the attacker. It is dependent on such factors as a) the strength and motivation of the attacker; b) their strategic situation; c) the intensity of the conflict; d) the type of

[94] Several months later, March 2, 2021, the Union Power Minister R. K. Singh stated that the power outage had been caused by human error and that there was "no evidence" that the attack had been caused by China. Governments and utilities often routinely deny or cover-up cyber-attacks as they are reluctant to acknowledge vulnerabilities.

[95] The Indian power companies were not specific regarding the details of their counter-measures.

[96] The Indians did not pay. They simply suspended services for 3-4 days while they rebuilt their IT system.

effect sought, *e.g.*, either tangible or primarily symbolic; and e) the co-dependency of the cyber-attack with other events.

Non-State Actors Have Limited Means But Can Do Substantial Damage

The Non-State Actor does not have the capabilities of a superpower, or of any Nation State.[97] It lacks the engineering skills, money, and infrastructure to develop a cyber-weapon as complex and sophisticated as Stuxnet. This paucity of resources available to devote to a cyber-attack means that it will be more difficult to engage in that comprehensive cyber-intelligence work needed to choose a target and determine its vulnerabilities. Without automatic network scanning capabilities, it would be problematical to pre-position logic bombs into the American electrical grid. In addition, it would be much more challenging to assemble the resources and skills needed for systems development of a sophisticated cyber-weapon such as StuxNet. This would make it difficult to create a device-specific attack.

This leaves us to expect that a Non-State Actor cyber-attack against the electrical grid of the United States would have the following characteristics: a) It would be organized by a small team; b) There is a high probability that the attack would take place on-site instead of remotely; c) Social engineering and recruitment of fellow-travelers might well be used to gain site access and to collect intelligence; d) Attacks are more probable against Civil Society targets instead of against the military because (i) there is a perceived lesser change of devastating retaliation; and (ii) attacks against Civil Society targets have a larger psychological and propaganda effect; e) The ability to attack the entire electrical grid of the United States is non-existent, consequently attacks would at most be against a regional facility, although multiple attacks, perhaps 2–3, might be launched in different locations at the same time.

In sum, cyber-attacks by Non-State Actors against the entire electrical grid are an unlikely event; any attacks against regional (or city) electrical grids from a cyber point of view are more probable but would be unsophisticated and primitive.

Iran Has A Proven Record Of Large Cyber-Attacks

The capabilities of Iran for conducting a cyber-attack are considerably better than those of the rag-tag bands of terrorists and revolutionary brigades mulling around the world. For a small country, it has scored a few notable cyber-attacks, including the highly-successful "Shamoon" attack in 2012 against Saudi Aramco and Qatar's RasGas. Also known as W32.DistTrack, the computer virus scooped up valuable files, transmitted them to the attacker, erased all of the data on the infected system, then wiped out its master boot record, making it impossible to re-start those computer workstations running Saudi Arabia's national oil company. The attackers claimed to be the "Cutting Sword of Justice." More than 30,000 workstations were wiped clean. The attack had been timed to coincide with Ramadan, so there were less personnel on site, allowing the malware to spread more extensively without being detected. Note that this timing was generally contextual in nature, and thus did not require extensive intelligence-gathering *inside* the targeted facilities.

[97] If the Non-State Actors were acting on behalf of a Nation State, then we would consider this to be a Nation State attack.

This attack was successful, but also may show the limitations in Iranian skills, at least at that time: a) The attack was a general attack against workstations, and not directed at specific process control (SCADA) equipment, which would have required more sophistication in the engineering of the payload; b) Although wiping out the hard disks of workstations certainly qualifies as an attack, the most it accomplished was a week's delay while Saudi technologists restored the information infrastructure, implying that although the attack was an irritation, ultimately it did little harm; and c) The attackers publicized on PasteBin.com[98] the purpose of the attack and their motivation; this done before the attack took place, thus lessening or eliminating altogether the chances of anonymity.

Nevertheless, thus far, Iran has a proven cyber-attack record in: a) website defacement; b) data breach and theft; c) denial of service attacks; and d) destructive attacks, such as a "wiper" attack that will erase the victim's information systems. For example, apart from the Saudi Aramco (2012) attack, Iran has scored a number of attacks against the United States. These include: a) the 2014 attack against the Sands Casino in Las Vegas which destroyed data on its internal network;[99] b) a number of DDoS attacks against U.S. banks (Bank of America; Wells Fargo; PNC Financial; SunTrust Banks) between 2011 and 2013 (done under the name "Qassam Cyber Fighters"); c) massive information operations (influence activities) involving Twitter and Facebook between 2009 and 2019; d) cyber-espionage against the U.S. Department of Labor, and the Federal Energy Regulatory Commission; and e) access and manipulation of the SCADA systems of the Bowman Dam in Rye, New York in 2013. This latter attack indicates Iranian efforts to develop cyber-attack capabilities against critical infrastructure.

We can expect that an Iranian cyber-attack against the electrical grid of the United States would have the following characteristics: a) It likely would rely on use of relatively indiscriminate tools for access that could be employed from a distance, such as the use of phishing emails; b) Iran would focus on information systems disruption and then rely on the secondary effects against the deeper infrastructure of the electrical grid, rather than attempting to cause those secondary effects itself; c) Iran's most probable attack point using cyber would be low-criticality services such as those market systems involved in the buying and selling (brokering) of electricity; d) Iran's progress in science and technology[100] would suggest it has the technical capabilities to target high-criticality systems such as Supervisory Control and Data Acquisition Systems (SCADA) or medium-criticality systems such as Substation Automation or Energy Management Systems;[101]

[98] "We ... an anti-oppression hacker group ... want to hit the ... Al-Saud corrupt regime [that has] ... hands ... infected with the blood of innocent children and people."

[99] The owner (53%) of the Sands Casino at the time was Sheldon Adelson (1933–2021), a supporter of Israel.

[100] In 2013, 1,505,030 engineering students in university; 509 doctorates produced in 2012 (latest data); exceeds Turkey in number of scientific (refereed) publications cited (2008-2012); around 40 scientific industrial parks. *Source*: UNESCO Science Report: Towards 2030 (2015). In addition, the Government of Iran has developed a number of offensive cyber capabilities including the IRGC Electronic Warfare and Cyber Defence Organization; Basij Cyber Council (paramilitary cyber force); Cyber Defence Command; Ministry of Intelligence and Security (MOIS), similar to the U.S. National Security Agency (NSA) and Islamic Revolutionary Guard Corps (IRGC) with overseas cyber activities.

[101] Iran has by now had a chance to reverse-engineer the StuxNet.

e) Iran has a moderate chance of inflicting temporary but substantial damage to the electrical grid, primarily in its supporting information processing operations; f) It is unlikely that Iran would be capable of attacking the entire electrical grid of the United States.

In sum, Iran can be a serious irritant against the electrical grid, but does not have yet the capability of launching a coordinated nation-wide cyber-attack. Iran should be considered capable of doing substantial damage to secondary processes associated with electricity generation.

It is expected that under current U.S. policy, Iran will develop thermonuclear weapons within half a decade or so along with the missile capabilities necessary for their delivery. As such, Iran theoretically could explode such a weapon in the atmosphere over the United States causing an electromagnetic pulse (EMP) to harm significant portions of the electrical grid. It is assessed that: a) Iran has the technical understanding of how to employ EMP effects generated from setting off atomic bombs in the atmosphere and continues to seek acquisition of an EMP device that might be used, providing it could get it delivered into the United States; b) Iran continues to work hard to develop cyber exploits into the U.S. electrical grid and has been successful in the implantation of malware; c) In spite of its relentless jingoistic posturing, Iranian leadership would be cautious of the response from the United States, which without question would react forcefully.

In Cyber, China Is A Mortal Threat To The United States

The People's Republic of China appears to be the world's leader in cyber-espionage, at least if measured by volume of pilfered information.[102] In addition, it is the world's largest manufacturer and consumer of electrical power and electrical equipment. It is reasonable to assume that in the course of China's R&D on electrical grid systems, it has conducted extensive technical research (patent analysis; tear-downs of foreign-manufactured equipment; evaluation of operational procedures; industrial espionage of newer technologies). In addition, after the Gulf Wars, China's military establishment adopted a "crash" program to develop cyber capabilities. China also has sent to the United States many scientists who have penetrated the control chambers of America's electrical grid operators. This access has given China's agents numerous opportunities to collect extensive intelligence on the U.S. grid, including both operating and recovery procedures as well as characteristics (specific machine and hardware identities) of its supporting ICT control systems.

China has the money, national laboratory network, trained personnel, and strategic necessity to develop the highest quality cyber-weapons capable of severely disrupting the electrical grid throughout the United States. The Chinese diaspora in the United States has placed potential Chinese agents[103] into virtually every part of the engineering and R&D associated with the electrical grid. In addition, China is not deterred from hitting the United States, as seen in the massive cyber-attack launched in retaliation for the April 2011 collision between a U.S. intelligence platform and a Chinese jet. The Chinese pilot flew recklessly close to the U.S. aircraft

[102] *See* "We assess that China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities ... [and] can cause localized, temporary disruptions to critical infrastructure within the United States" ODNI 2021 Rpt. p. 8, para. 5-6

[103] The Government of China uses the extended family remaining in China to coerce cooperation from family members living in the United States, even if they are U.S. citizens.

and was said to have crashed, killing the pilot, although the death was not confirmed.[104] Shortly thereafter, the United States suffered a number of massive cyber-attacks. These were organized and supported by the Government of China, although under the laughable fiction they were "spontaneous" actions of patriotic and concerned Chinese citizens. The attacks, motivated by such slogans as "Hack it Great Chinese!!", and hastily constructed web-sites such as KillUSA.com were meant to serve as a warning to the United States.

Another factor in understanding the danger of cyber-attacks made by China is the contextual framework of its overall strategy, or lack of one. In the past half-decade, Chinese diplomacy has done what no other nation was capable of doing: It stimulated formation of a cooperative alliance-like system between Japan, India, Vietnam, South Korea, The Philippines and others aimed at resisting Chinese hegemonic expansionism. These countries combined have more population, more technology, and more money than China.[105] Rather than physical confrontation, China prefers as a default use of "soft power," *e.g.*, propaganda and corruption of elites by bribery. In Texas, Chinese owned corporations have purchased very large tracts of land and are setting up wind-farms to take advantage of subsidies for green energy paid by the U.S. government. As such, we can expect there will be no let-up of intensive cyber-espionage conducted by the Chinese government itself against the United States and its industries, including the electrical grid.

We can expect that a cyber-attack by China against electricity in the United States would have the following characteristics: a) China has the capability to disable all or at least very large parts of the electrical grid (Eastern, Western, Texas Grid Interconnects) as well as target specific areas, such as power in a single metropolitan area; b) A massive cyber-attack against the entire electrical grid would take place within the context of a general war between the United States and China, but a large-scale conventional or nuclear war is highly unlikely; c) More likely is a massive cyber-attack against the entire U.S. electric grid prior to the outbreak of conventional or nuclear war, or during an extreme international crisis, to deter or defeat the U.S. with "gray-zone aggression" instead of or prior to outbreak of a "real shooting war" consistent with China's military doctrine that Cyber Warfare is an unprecedented and decisive Revolution in Military Affairs; d) China is prepared to use targeted attacks against America's electrical grid as a stand-alone method of fighting what it calls "U.S. Hegemony"; e) There is a moderate chance of some irritating event such as an accidental boat collision on the high sea leading to a repeat of the Hainan Island incident, leading to another fabricated "patriotic" cyber-attack against the United States, perhaps against a small portion of the electrical grid (but not against the entire system, and only if there was significant loss of Chinese life in the incident); f) China might engage in a cyber-attack against electrical grid systems of low-criticality as a symbolic warning if it feared an attack from the United States; g) China may engage in brokering of vulnerability information about the electrical grid in the United States as an unscrupulous profit-making activity, with exploits being sold to Non-State Actors or nations such as Russia.

---

[104] *See* Shirley A. Kan, et al., China-U.S. Aircraft Collision Incident of April 2001: Assessments and Policy Implications CRS Report for Congress, No. RL30946 (10 October 2001).

[105] *See* extensive discussion and analysis in Edward N. Luttwak, *The Rise of China vs. the Logic of Strategy* (Cambridge: Belknap Press, 2012).

Russia Is The Best Prepared To Defend Against Cyber-Attack And Use Cyber As A Strategic Weapon

Russia does not have the amount of money or human resources of China but it does have superior strategy-making capabilities. In addition, Russia has a long-proven track record of being able to develop world-class offensive capabilities in any field using a fraction of the resources of the United States. Russia does not brag and publicize its cyber warfare capabilities as does the United States, but from examination of publicly available documents, we know that if needed, it can closely integrate its military with all resources in civil society, including all of its hackers.[106]

Russian cybersecurity companies routinely monitor the world's Internet, and are sensitive to any threats. Unlike the United States, Russian law passively encourages development of robust hacking skills because it is not illegal for its citizens to hack computing resources *outside* in other countries.[107] Finally, Russia has a reliable habit of *always* launching a counter-strike if it has been attacked, and this includes in the cyber domain.[108]

We can expect that a cyber-attack by Russia against the electrical grid of the United States would have the following characteristics: a) Russia is capable of launching a massive attack that would shut down in one coordinated attack at least 80% of America's electrical grid; b) Russia has developed the capabilities of attacking high-criticality SCADA systems in the electrical grid, as well as all other systems; c) Russia likely knows more about EMP than the United States given its extensive testing and development of EMP weapons;[109] d) A massive Russian attack against the entire electrical grid would occur within the context of a major strategic conflict between Russia and the United States; e) During an extreme international crisis, a massive Russian cyber-attack against the entire U.S. electric grid prior to the outbreak of conventional or nuclear war is likely, to deter or defeat the U.S. with "gray-zone aggression" instead of or prior to outbreak of a "real shooting war" consistent with Russia's military doctrine that Cyber Warfare is an unprecedented and decisive Revolution in Military Affairs; f) Russia's response to a major cyber-attack made by the United States is likely to be at least proportional but more likely disproportional and massive, possibly even resulting in Russian nuclear retaliation as threatened in their military doctrine; g) Like China, Russia possibly would use a targeted cyber-attack against a low-criticality electrical grid system as a show of force and warning to deter escalation in a conflict by the United States; h) Russia likely has experimented with placement of cyber logic-bombs in portions of America's

---

[106] *See* ODNI 2021 RPT. p. 10, para. 8-9 ("Russia will remain a top cyber threat ... [and] continues to target critical infrastructure, including underwater cables and industrial control systems ... [giving it] ability to damage infrastructure during a crisis").

[107] The criminal system in Russia successfully deters Russian hackers from applying their skills against Russian targets.

[108] For example, recent discussion of Russian interference in the U.S. election system rarely mentioned the preceding use of the Internet and social media by the United States as official policy to influence events inside Russia.

[109] *See* reports of the 1961 testing in Russia at Vasily N. Greetsai, Andrey H. Kozlovsky, Vadim M. Kuvshinnikov, Vladimir M. Loborev, Oleg A. Parfenov, Oleg A. Tarasov, and Leonid N. Zdoukhov "Response of Long Lines to Nuclear High-Altitude Electromagnetic Pulse (HEMP)" 40 IEEE Transactions on Electromagnetic Compatibility pp. 348–354 (1998).

electrical grid; i) Russia is more capable than other countries in placement of assets (human agents) into critical parts of the management structure of the American electrical grid.

For U.S. relations with both nations, Russia and China, the emergence of viable paths to cyber-attacks against critical infrastructure as a new strategic weapon has lowered the barriers to conflict, and presents a heightened danger with the potential to disrupt the long-standing balancing calculus dependent upon nuclear deterrence.

PHASE	SCALE OF CYBER ATTACK AGAINST ELECTRICAL GRID		CHINA	RUSSIA	IRAN	NON-STATE ACTOR (TERRORIST)
INTELLIGENCE (TARGET SELECTION)	CYBER ESPIONAGE	NETWORK MAPPING	YES	YES	YES	NO
		DEVICE IDENTIFICATION	YES	YES	NO	NO
PREPARATION	ENGINEER MALWARE		YES	YES	NO	NO
	PRE-POSITION LOGIC BOMBS		YES	YES	NO	NO
SITE ACCESS	SOCIAL ENGINEERING ATTACK		YES	YES	NO	YES
	ZERO DAY EXPLOITS		YES	YES	YES	NO
ATTACK	KINETIC ATTACK	KINETIC ATTACK	NO	NO	NO	YES
		DEVICE SPECIFIC	YES	YES	NO	NO
	STAND ALONE CYBER ATTACK	INFORMATION OPERATIONS	YES	YES	NO	NO
		MASS BRIGADE	YES	NO	NO	NO
		DDOS AND SIMILAR	YES	YES	YES	YES
	IN TANDEM WITH CONVENTIONAL OR NUCLEAR FORCES	MILITARY TARGET	YES	YES	NO	NO
		CIVIL SOCIETY TARGET	YES	YES	NO	YES

TABLE 1 PHASES OF CYBER ATTACK AND CAPABILITIES OF ATTACKERS

LEVEL OF CRITICALITY	CYBER VULNERABILITY POINTS IN THE ELECTRICAL GRID	
HIGHEST	SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEMS (SCADA	REAL-TIME MEASUREMENTS FROM SUBSTATIONS
		SEND CONTROL SIGNALS TO EQUIPMENT (CIRCUIT BREAKERS; OTHER CONTROL SYSTEMS)
MEDIUM	SUBSTATION AUTOMATION SYSTEMS	CONTROL OF LOCAL EQUIPMENT
	ENERGY MANAGEMENT SYSTEMS	REAL TIME ANALYSIS OF RELIABILITY OF SYSTEMS
LOW	MARKET SYSTEMS	BUYING AND SELLING OF ELECTRICITY

TABLE 2 LEVELS OF CRITICALITY FOR INFORMATION SYSTEMS IN THE ELECTRICAL GRID

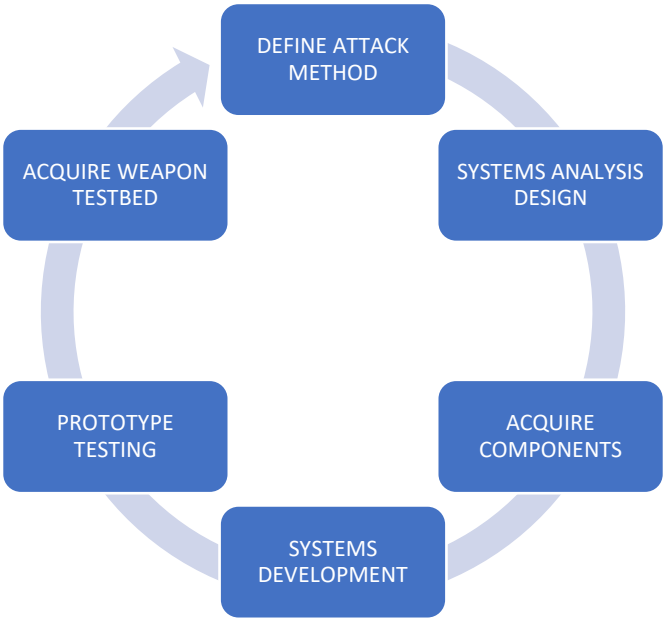

FIGURE 1 SYSTEM DEVELOPMENT CYCLE FOR MALWARE

SUPPLEMENTARY ROLE FOR CYBER	NUCLEAR AND CONVENTIONAL WEAPONS	WARFARE BETWEEN NATION STATES; CYBER IN SUPPORTING ROLE TO ASSIST IN TRADITIONAL COMBAT
CYBER-ONLY OPERATIONS	CYBER KINETIC ATTACKS	CYBER ATTACKS DESIGNED TO HAVE REAL-WORLD PHYSICAL CONSEQUENCES; NEW AND DANGEROUS REALM OF NATION-STATE CONFLICT
	INFORMATION OPERATIONS	USE OF CYBER FOR INJECTING PROPAGANDA OR MANIPULATING SOCIAL MEDIA AND THE POLITICAL MOVEMENTS DEPENDENT UPON IT.
	CYBER ESPIONAGE	PASSIVE COLLECTION OF GOVERNMENT, MILITARY, AND COMMERCIAL INFORMATION. MONITORING OF ONE'S NATIONALS LIVING IN OTHER NATION STATES.

TABLE 3 CYBER KINETIC ATTACKS REPRESENT POTENTIALLY A NEW FORM OF WARFARE BETWEEN NATION STATES

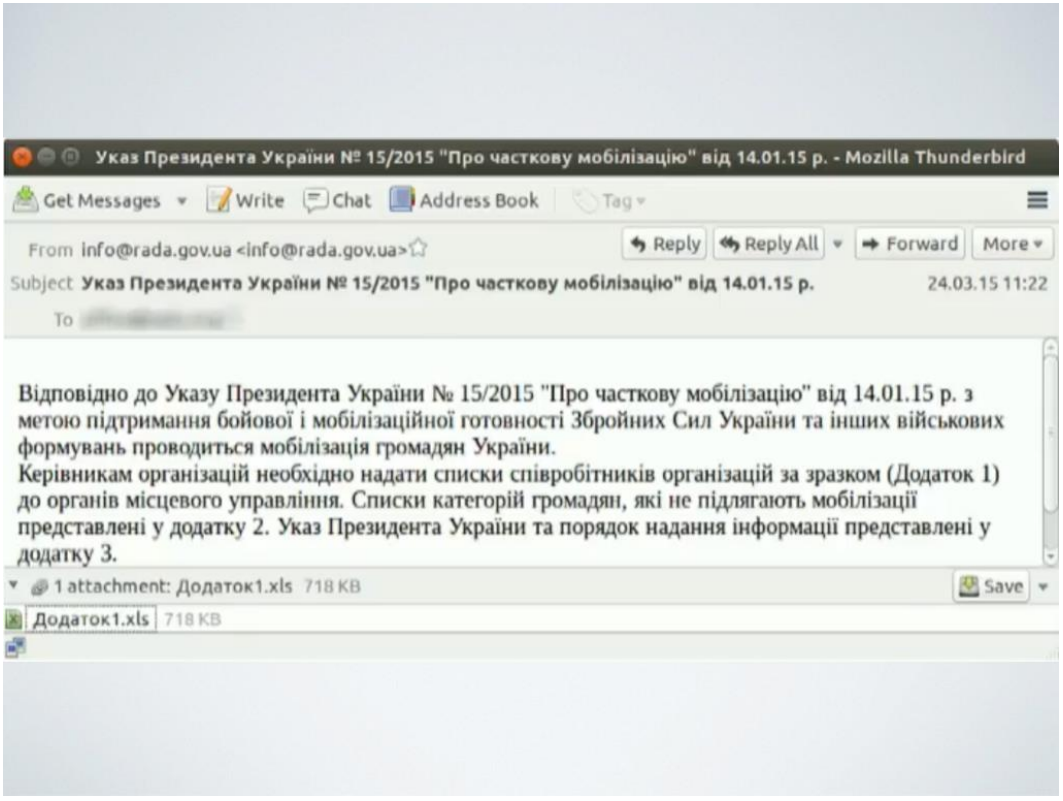

FIGURE 2 A COPY OF THE PFISHING EMAIL SENT TO THE UKRANIAN GRID OPERATORS (THE LANGUAGE APPEARS AS MIGHT AN OFFICIAL GOVERNMENT DOCUMENT)

Dr. Edward M. Roche Ph.D., J.D.

Ed received an M.Phil and Ph.D. in Political Science from Columbia University with a concentration in Diplomatic History, International Law, and African Political Economy. He earned an M.A. in International Relations from the Johns Hopkins School of Advanced International Studies (SAIS) in Washington, D.C., and has a Certificate with Distinction in European Law from the University of Leiden, a Certificate with Distinction in Management of International Organizations from the University of Geneva, and a Certificate in Molecular Neuropharmacology from the California Institute of Technology. He is certified in Russian and Chinese. Ed is a member of the California Bar Association, the American Society of International Law, the FBI InfraGard partnership cybersecurity group, and Affiliate Researcher for the Columbia Institute for Tele-Information at Columbia Business School. He has served with the United Nations as a Program Evaluator and Expert on e-Government and Internet Governance as well as Expert Advisor for national ICT innovation strategies in Central Asia and Africa. Prior to his work at the UN, he served as Chief Research Officer of the Research Board (Gartner) where he led multi-client research for Chief Information Officers on international technology management and cyber security. He is a member of the Association of Former Intelligence Officers (AFIO) and has consulted on Virtual Worlds and Virtual Reality for the Intelligence Advanced Research Projects Activity (IARPA) and Office of Disruptive Technologies. He wrote the chapter on Industrial Espionage for the AFIO publication *Guide to the Study of Intelligence* and also published *Snake Fish: The Chi Mak Spy Ring and Chinese Industrial Espionage* and *Corporate Spy: Industrial Espionage and Counterintelligence in the Multinational Enterprise*. He also published the seminal book *Managing Information Technology in Multinational Corporations*, "International Convention for the Peaceful Use of Cyberspace" (*Orbis*, 2014) and "La course au cyber armament" (*Netcom*, 2019). Ed taught at the Grenoble Ecole de Management from 2009-2016. He did research for Edward Luttwak for the appendix to the book *Coup d'Etat* and consults on wireless broadband and 5G network strategies for telecommunications providers. He monitors the Cyber Stability work of the UN First Committee on Disarmament, and does analysis of cyber weapons, the cyber arms race, and national strategies for a new arms control convention to manage cyber conflicts. He has published on development of an International Cyber Peacekeeping Force. Ed lives in New York City and can be reached at emr96@columbia.edu.